KPMG

# Cyber Security: Purple Teaming service

## A KPMG Service for G-Cloud 15

# KPMG – About us

## Our UK Cyber team

We've worked with countless organisations across multiple sectors, including financial services, life sciences, healthcare, government, telecommunications, energy and natural resources, and legal services. Our clients range in sizes, span across geographies and industries and are subjects to various regulatory requirements and obligations.

330+ professionals

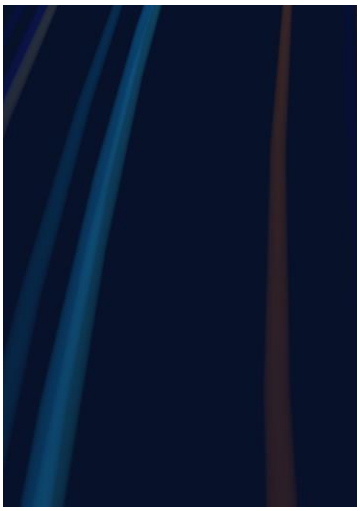
15 office locations

Part of a global team of 6200+ individuals

## Our services

UK Cyber operates across 8 different service lines, catering to a wide range of governance and technical needs.

| | |
|---|---|
| Cyber strategy | Cyber and enterprise resilience |
| Cyber tech transformation | Cyber defence services |
| Cyber risk | Privacy compliance |
| Identity and access management | Cyber incident response |



### Our Cyber team is complemented by our Connected Technology team.

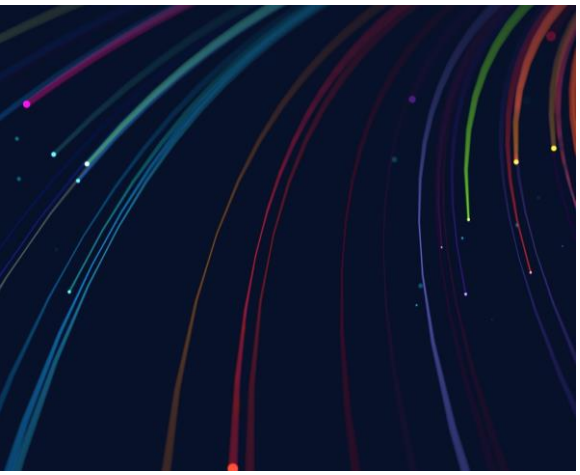
We have access to a 2000-strong team of client-facing technologists combined with alliance partners, with a diverse range of skills and experience. This enables us to bring to our clients the most suitable resources, expertise and insights when needed.

We apply a data and technology driven approach to drive change through our digital transformation services.

# Cyber Security: Purple Teaming service

## Service Description

KPMG delivers collaborative Purple Teaming exercises for a range of clients across the public sector organisations in the UK and globally. Our Purple Teaming service simulates realistic cyber threats to exercise and enhance your SecOps capability, across prevention, detection, and response. We establish a safe and collaborative learning environment, enabling upskilling of Blue Team personnel and identifying strategic and tactical recommendations for improvement, with considerations across people, process and technology.



## What are the benefits of KPMG Purple Teaming?

- Optimised alerting and detection capability
- Improved collaboration between Security and IT teams
- Enhanced response processes and playbooks
- Strategic prioritisation of improvement activities
- Increased security awareness across the organisation
- Improved insight into emerging issues and solutions to ever-increasing threats

## Our service features

- Simulate realistic threat scenarios, tailored to your organisation
- Combined Red and Blue Team expertise
- Vulnerability identification and prioritisation
- Security response optimisation, both tactically and operationally
- Collaborative learning environment and upskilling workshops
- Social engineering activities to exercise your employees' security awareness

# Purple Teaming: Our Approach

## Overview

Cyber Security incidents are increasingly unpredictable in both their targets and their methods. KPMG combines field-leading expertise collaborative exercising to define and carry out realistic scenarios to help achieve actionable and relevant insights, keeping your organisation secure.

- Cyber security breaches are today more common and ever more public. Threat agents such as hacktivists, organised crime groups and state-sponsored cyber spies have a variety of motivations and almost any organisation can be a potential target.
- While organisations are already struggling to maintain a clear view of their complex and widely distributed IT environments, the traditional security assurance activities are not answering the fundamental question – how well equipped are we to handle a cyber attack?
- We can help refine your requirements, define and carry out realistic cyber security scenarios that combine breadth-first target identification, target prioritisation, and in-depth focus on your key problem areas.

## Introducing Purple Teaming services

- Purple Teaming simulates realistic cyber threats to dynamically test technical controls and exercise cyber response capabilities. Unlike traditional red and blue team exercises which operate independently, purple teaming fosters collaboration and communication between the two teams.
- This allows for a more realistic and dynamic simulation of real world attacks, enabling organisations to exercise prevention, detection and response capabilities more effectively, and identifying strategic and tactical opportunities for capability enhancement.
- We have helped many Government Departments and public sector organisations enhance their defensive cyber capability through Purple Teaming.

## What's in the box

Our Purple Teaming services provide you with a collaborative learning opportunity to upskill your Cyber and IT teams and enhance your technical and operational cyber response capability.

We will work with you to define priority threat scenarios and test cases relevant to your organisation, carry these out with consideration to the operational impact, and clearly explain the discovered vulnerabilities and their business impact. We will execute those test scenarios through a combination of manual and automated techniques to give you breadth and depth of coverage.

We support daily collaboration with your security and IT teams, with workshops designed to promote collaboration and continuous improvement.

- Simulating the actions of a hacker aiming to breach your organisation from the internet
- Working with you to explore opportunities to enhance your detection and response capabilities, providing tailored tactical, operational and strategic recommendations.

## One recent Government client said...

**We really enjoyed getting to work with the team over the course of the engagement and the output has been exceptionally helpful in giving some external assurance of our current position and the people, processes & technology that is in place, as well as clearly identifying areas that need development and maturing. The recommendations that we've begun implementing are already reaping a benefit and have led to detections that would previously have been missed.**

# Service Details

## Pricing overview, including volume discounts or data extraction costs

Consulting Prices are as per the G Cloud 14 rate structure.

Projects can be charged using either Fixed Price and Time and Materials approaches, according to the situation, and can be delivered on site and/or remotely.

Volume discounts would be considered on a case by case basis.

Data extraction is not included in this service.

## Service constraints like maintenance windows or the level of customisation allowed

This is not relevant to this service.

## Service levels like performance, availability and support hours

Not relevant to this service.

## How you'll repay or compensate buyers if you do not meet service levels

Any service credit regime for Cloud software vendors are per the relevant authority's direct agreement with that vendor.

KPMG can discuss specific service credit requirements on a case by case basis.

## The ordering and invoicing process

The ordering process for G Cloud services is laid out in the 'G Cloud buyers' guide on the www.gov.uk website.

Invoicing arrangements will be as per the agreed G Cloud order form and will vary from engagement to engagement.

## How buyers or suppliers can terminate a contract:

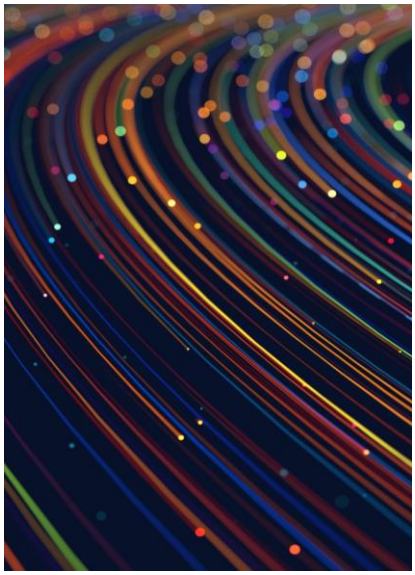
Our terms provide for a range of scenarios where both Buyer and Supplier are able to terminate contracts, to defined notice periods, for:

- convenience,
- failure to remedy a material breach, and
- insolvency.

In addition, Supplier has the right to terminate if: (a) circumstances arise or have arisen which KPMG reasonably considers does or may impair its impartiality, objectivity or independence in respect of the provision of the Services; or (b) for legal, regulatory or other justified ethical reasons.

## After sales support

KPMG can provide a range of services to assist users of this service post implementation ranging from managed services, staff secondment, impact assessments on the implementation due to cloud software vendor upgrade / major patches and associated regression testing.



## Any technical requirements

In the event of supplying software services, each cloud software vendor provides details directly of their supported web browsers and personal computer and related requirements. These are not onerous and typically do not present an issue for the majority of organisations.

KPMG also uses a range of collaboration tools, as appropriate, to assist in the delivery of the Services. Microsoft Office 365 & Teams plus Skype are used by all colleagues within the firm, with other tools such as Jira and Confluence being used if required for the project. KPMG is also able to use other collaboration tools if used on client provided laptops.

Project team members will need to be provided with a software VPN and virtual machine or client laptop.

kpmg.com/uk



**Document Classification: KPMG Confidential**

CREATE. | CRT164925A January 2026